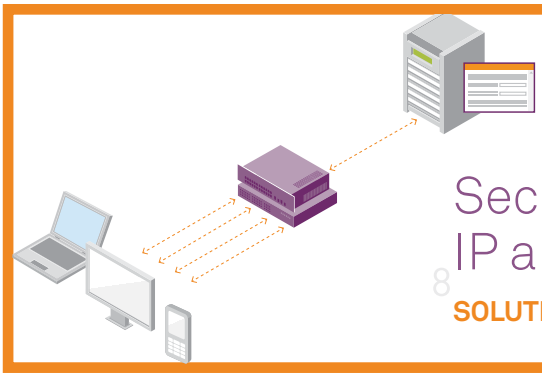
SafeNet | THE DATA PROTECTION COMPANY



# Secure Your Network Traffic with F5 BIG-IP and SafeNet Luna SA

**SOLUTION BRIEF**

## Key Benefits

### Virtual editions available for the cloud

BIG-IP and Luna SA are available for deployment in enterprise, private, hybrid and public clouds. The AWS CloudHSM service is powered by SafeNet Luna SA while BIG-IP is available in AWS Marketplace in a virtual edition.

### High performance processing

Luna SA HSMs are capable of processing up to 7,000 RSA and 1,000 ECC transactions per second. High processing speeds allow administrators to offload cryptographic functions to improve datacenter performance.

### Robust security

Luna SA HSMs offer the highest level of tamper resistance and security, and have been validated to be compliant with FIPS 140-2 Level 3 and Common Criteria EAL 4+ standards.

### Meet compliance standards

High assurance hardware key storage is an important part of meeting data governance requirements. Luna SA's high performance and top of the line security make demonstrating compliance easier.

Downtime for corporate applications delivered through networks is not an option. Since organizations use these applications to generate revenue and manage operations, disruption and compromise directly impacts the bottom line. With the stakes so high, securing these resources and ensuring their availability is essential. Sophisticated attacks – such as Distributed Denial of Service attacks – can disrupt the availability of corporate applications or compromise the sensitive data traveling within a network. Protecting these resources is required to protect an organization's success.

## The Solution: BIG-IP and Luna SA

SafeNet Luna SA HSMs integrate with BIG-IP's Local Traffic Manager (LTM) and Access Policy Manager (APM) to secure the network over which BIG-IP delivers applications. Luna SA stores the certificates and encryption keys at the heart of BIG-IP's SSL transactions. LTM and APM intelligently deliver applications from best-performing data centers to authorized users in an effort to optimize network resources according to pre-defined business policies. SafeNet ensures that the network activity managed by BIG-IP occurs in tunnels secured by robust encryption and server authentication.

### F5 BIG-IP Local Traffic Manager

BIG-IP Local Traffic Manager (LTM) is a high performance application delivery system that intelligently manages network traffic in order to optimize performance. Its ability to balance loads and offload cryptographic operations eliminate single points of failure while maintaining security and high performance. LTM's ability to manage traffic across physical, virtual and cloud environments makes it easy to move applications across cloud and traditional physical architectures.

### F5 BIG-IP Access Policy Manager

BIG-IP Access Policy Manager (APM) is a flexible, high-performance access and security solution that consolidates remote and LAN access, as well as wireless connections within a single management interface. APM unifies access to corporate applications and networks, and controls entry to those unified resources through easy-to-manage access policies. When LTM centralizes application delivery and adds BIG-IP APM, enterprises simplify the implementation of authentication and authorization controls ultimately protecting the organization from unauthorized access and sophisticated attacks.

### SafeNet Luna SA HSM

Luna SA HSMs are robust, high-availability, and high-performance appliances that store cryptographic materials (e.g. certificates, encryption keys, etc.) in a secure FIPS 140-2 Level 3 tamper-proof hardware appliance. Storing these materials in a hardware appliance keeps them out of harm's way and ensures that only authorized administrators have access to important encryption keys. With Luna SA as a security infrastructure's trusted root, administrators can ensure the integrity of their cryptographic operations.

Secure the transport layer while improving datacenter performance.

BIG-IP stores, processes and encrypts both keys and data in Luna SA hardware security modules. By offloading these cryptographic functions from general servers, Luna SA frees valuable compute resources. Capable of performing thousands of cryptographic transactions per second, Luna SA offers the throughput and responsiveness to serve as an SSL accelerator supporting the most demanding SSL operations. Not only does Luna SA secure valuable encryption materials in a tamper-proof appliance, it adds value to any environment by taking on resource intensive cryptographic operations which improves overall datacenter performance.

## Key features

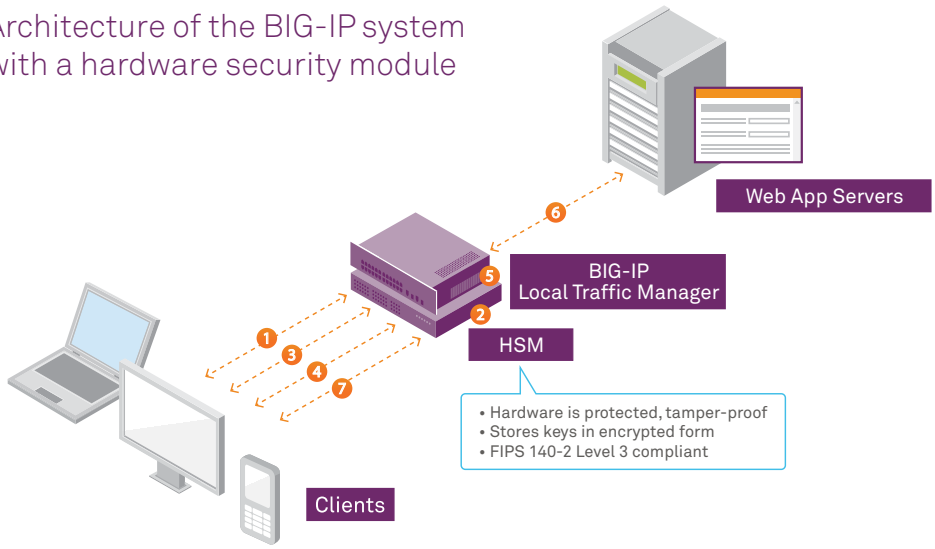
### Robust security

BIG-IP stores in Luna SA HSMs the private keys and associated certificates used by BIG-IP LTM to authenticate servers involved in SSL transactions. With Luna SA as the root of trust, organizations can securely send data and deliver applications through protected SSL tunnels. Data is encrypted before it travels and the keys necessary to decrypt it never leave the hardware appliance thus eliminating the possibility that data will be intercepted while in clear text. Together, the solution mitigates risk from attacks by both deflecting them as they come and securing the internal resources so there is nothing left to see if a breach occurs.

### High availability

BIG-IP LTM ensures high availability by redirecting traffic to separate, functioning datacenters in the case of a site's disruption. Because BIG-IP ensures that there can be no single point of failure, applications remain persistently accessible. As a complement, multiple Luna SAs can be configured for high availability so encryption keys are always available to secure SSL transactions. Multiple HSMs can be grouped in high availability configurations to scale performance to process tens of thousands of transactions per second. Luna SA's integration in BIG-IP environments ensures that encryption keys and certificates are always protected and available to identify servers and secure the transport layer.

### Architecture of the BIG-IP system with a hardware security module




1. Client requests a page with SSL
2. BIG-IP LTM retrieves public key
3. Server responds with public key
4. Client creates a symmetric key and sends it to BIG-IP LTM
5. BIG-IP LTM decrypts the symmetric key using its private key
6. BIG-IP LTM retrieves page from app server
7. Client and BIG-IP LTM communicate using the symmetric key

## Conclusion

SafeNet and F5 join together to secure and optimize the delivery of corporate applications. With Luna SA, organizations can trust that the data traveling in its BIG-IP managed network is encrypted and secure from unauthorized users. Whether the attack is aimed at denying service or stealing valuable data, the BIG-IP/Luna SA solution provides a high-performance, robust and reliable answer for security administrators. For more information visit: http://www.safenet-inc.com/partners/f5

**Contact Us:** For all office locations and contact information, please visit **www.safenet-inc.com**
**Follow Us:** www.safenet-inc.com/connected